Almost Perfect Nonlinear functions

Thierry Pierre Berger, Anne Canteaut, Pascale Charpin, Yann Laigle-Chapuy

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Almost Perfect Nonlinear functions

Thierry P. Berger — Anne Canteaut — Pascale Charpin — Yann Laigle-Chapuy

N° 5774

Décembre 2005

THÈME 2

ISSN 0249-6399 ISRN INRIA/RR--5774--FR+ENG

Almost Perfect Nonlinear functions

Thierry P. Berger [*] , Anne Canteaut[†] , Pascale Charpin[‡] , Yann Laigle-Chapuy[§]

Thème 2 — Génie logiciel
et calcul symbolique
Projet Codes

Rapport de recherche n° 5774 — Décembre 2005 — 28 pages

Abstract: We investigate some open problems on Almost Perfect Nonlinear (APN) functions over a finite field of characteristic 2. We provide new characterizations of APN functions and of APN permutations by means of their component functions. We generalize some results of Nyberg (1994) and strengthen a conjecture on the upper bound of nonlinearity of APN functions. We also focus on the case of quadratic functions. We contribute to the current works on APN quadratic functions, by proving that a large class of quadratic functions cannot be APN.

Key-words: Boolean function, Almost bent function, almost perfect nonlinear function, power function, permutation polynomial

An extended abstract of this paper was published in the proceedings of *2005 IEEE International Symposium on Information Theory*, ISIT 05, Adelaide, Australie, September 2005.

A short version of this paper will be published in *IEEE Transactions on Information Theory.* The authors would like to thank the anonymous reviewers who, by numerous comments and suggestions, have contributed to improve the manuscript.

[*] LACO, Faculté des Sciences de Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex, France. e-mail: thierry.berger@unilim.fr

[†] INRIA, Domaine de Voluceau-Rocquencourt, BP 105 - 78153, Le Chesnay, France. e-mail: Anne.Canteaut@inria.fr

[‡] *idem*, e-mail: Pascale.Charpin@inria.fr

[§] *idem*, e-mail: Yann.Laigle-Chapuy@inria.fr

Fonctions presque parfaitement non linéaires

Résumé : La sécurité des *systèmes de chiffrement symétriques* repose en grande partie sur les propriétés des fonctions booléennes qu'ils utilisent. Les propriétés de ces fonctions sont en effet souvent cruciales lors d'attaques contre ce type d'algorithmes. Ainsi, dans le *chiffrement itératif par bloc*, l'efficacité de la plupart des cryptanalyses statistiques dépend essentiellement des propriétés de la fonction de substitution utilisée dans la fonction de tour. Cette fonction, appelée *boîte-S*, est une fonction vectorielle représentée par ses composantes booléennes.

Dans cette étude nous nous intéressons aux boîtes-S qui présentent la meilleure résistance aux *attaques différentielles* [3]. Le but d'une attaque différentielle est d'identifier des couples de textes clairs dont la différence est fixée, et dont la différence des images présente un biais spécifique hautement probable. Pour une boîte-S à n entrées représentée par une fonction F sur $\mathbf{F}_2^n$, la résistance à cette cryptanalyse est quantifiée par le paramètre $\delta(F)$:

$$\delta(F) = \max_{a \neq 0, b} \#\{x \in \mathbf{F}_2^n,\ F(x+a) + F(x) = b\}.$$

Une condition de sécurité est que la distribution des valeurs de toutes les dérivées de F soit proche de la distribution uniforme, c'est-à-dire que $\delta(F)$ soit le plus petit possible. Toute boîte-S F à n entrées et n sorties vérifie $\delta(F) \geq 2$. Les fonctions F telles que $\delta(F) = 2$ sont dites *presque parfaitement non-linéaires* (APN, *i.e.*, almost perfect nonlinear).

Les fonctions APN sont donc d'un grand intérêt en cryptologie puisqu'elles offrent une résistance optimale à la cryptanalyse différentielle, mais ce sont aussi des objets discrets exceptionnels. La recherche théorique sur les fonctions APN a pour domaine l'ensemble du codage binaire (*suites, codes correcteurs, polynômes ...*) La classification des fonctions APN est loin d'être achevée et de multiples problèmes d'un grand intérêt restent non résolus.

Nous étudions ici un certain nombre de ces problèmes ouverts. Nous donnons des éléments de caractérisation, principalement en généralisant les travaux de Nyberg [23, 24]. Nous apportons notamment des améliorations pour ce qui est de la non-linéarité des fonctions APN et de l'existence de permutations APN (lorsque le nombre de variables est pair). Nous donnons des éléments de description des *fonctions puissances* APN. Enfin, nous caractérisons une large classe de fonctions quadratiques qui ne peuvent être APN.

Ce dernier résultat apporte des éléments nouveaux pour élaborer une classification des fonctions APN quadratiques, et doit être placé dans le contexte de plusieurs travaux très récents, initiés par l'équipe d'A. Pott, qui mettent en évidence la première classe de fonctions APN quadratiques non équivalentes à des fonctions puissances (voir [4, 17],(2005)).

Mots-clés : fonctions booléennes, fonctions presque parfaitement non linéaires, fonctions presque courbes, fonctions puissances, polynômes de permutation.

1 Introduction

Most attacks on symmetric cryptographic algorithms are related to some properties of the Boolean functions describing the system. For iterated block ciphers, the efficiency of the main cryptanalytic techniques (such as linear cryptanalysis, differential cryptanalysis...) can be measured by some quantities related to the confusion part of the round function, usually named S(ubstitution)-box. This paper focuses on the S-boxes which guarantee a high resistance to differential cryptanalysis [3]. This attack successfully applies when two plaintexts with fixed difference lead after the last-but-one round to outputs whose difference takes a certain value with a high probability. Therefore, a necessary security condition is that the output distributions of all derivatives of the involved S-box, $x \mapsto F(x+a)+F(x)$, must be close to the uniform distribution. The relevant parameter for an S-box F with n inputs is then

$$\delta(F) = \max_{a \neq 0, b} \#\{x \in \mathbf{F}_2^n,\ F(x+a)+F(x) = b\}\ ,$$

which must be as small as possible. When the number of output bits of the S-box is the same as the number of inputs (this is the case in most ciphers), we have that $\delta(F) \geq 2$, and the functions achieving this bound are called *almost perfect nonlinear (APN)* [25]. Therefore, APN functions are those S-boxes which offer optimal resistance to differential cryptanalysis.

As optimal objects, APN functions are also used in several other areas of telecommunications. Most notably, APN functions correspond to linear codes of length $2^n - 1$ and dimension $2n$ which have the best minimal distance 5 [11]. Thus, APN functions are of great interest in coding theory. Despite a number of recent works, many problems remain open. Actually, only a few APN functions are known, and most of them are affinely equivalent to a power function (see e.g. [5]). The first infinite class of quadratic APN functions, which are not equivalent to any power function, was exhibited very recently (see [4] and [17]). In this paper, we investigate some open problems on APN functions and we give partial results.

The next section gives some basic definitions related to APN functions over $\mathbf{F}_2^n$. Actually, in the whole paper, we identify the vector space $\mathbf{F}_2^n$ with the finite field $\mathbf{F}_{2^n}$ of order 2^n and such a function F is expressed as a polynomial in $\mathbf{F}_{2^n}[x]$. Since F can be represented by the collection of its n Boolean coordinates, we also recall some properties on Boolean functions. In Section 3.1, we study the APN functions by means of their Boolean components. We prove that the necessary condition for a function to be APN, introduced in [24], is also sufficient (Theorem 2). Then, we derive a new characterization of APN functions (Corollary 1). We later characterize APN permutations of $\mathbf{F}_{2^n}$ (Proposition 2). This last result is motivated by the conjecture that there is no APN permutation of $\mathbf{F}_{2^n}$ when n is even. In this context, and using our characterization, we prove that there is no APN permutation whose component functions are plateaued (Corollary 3 and Theorem 3). We also give a new characterization of APN power functions on $\mathbf{F}_{2^n}$ when n is even and an upper bound on their nonlinearity (Theorem 4). The last section is devoted to quadratic APN functions. It is well-known that the power functions of the form x^{2^k+1} over $\mathbf{F}_{2^n}$ with $\gcd(k,n) = 1$

are APN. But, the classification of quadratic APN functions which are not equivalent to the previous power functions is still an open problem. Here, we exhibit a whole subclass of quadratic functions which does not contain any APN functions. This result gives us more information about the form of quadratic APN functions (Proposition 7).

2 Definitions and basic properties

In this section, we introduce notation and some basic properties which will be used in all the paper. The next definition is general and then suitable for Boolean functions. Actually, in this paper, we treat the cases $m = n$ and $m = 1$ only.

Definition 1 *Let n and m be two nonzero integers. Let F be a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^m$. For any $a \in \mathbf{F}_2^n$, the* derivative of F with respect to a *is the function D_aF from $\mathbf{F}_2^n$ into $\mathbf{F}_2^m$ defined by*

$$D_aF(x) = F(x+a) + F(x), \quad \forall x \in \mathbf{F}_2^n \ .$$

If D_aF is constant then a is said to be a linear structure *of F.*

The resistance to differential cryptanalysis is related to the following quantities.

Definition 2 *Let F be a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^n$. For any a and b in $\mathbf{F}_2^n$, we denote*

$$\delta(a,b) = \#\{x \in \mathbf{F}_2^n, \ D_aF(x) = b\} \ ,$$

where $\#E$ is the cardinality of any set E. Then, we have

$$\delta(F) = \max_{a \neq 0, \ b \in \mathbf{F}_2^n} \delta(a,b) \geq 2$$

and the functions for which equality holds are said to be almost perfect nonlinear (APN).

The APN property can be equivalently defined as follows.

Proposition 1 *Let F be any function on $\mathbf{F}_2^n$. Then, F is* almost perfect nonlinear *(APN) if and only if, for any nonzero $a \in \mathbf{F}_2^n$, the set $\{D_aF(x), x \in \mathbf{F}_2^n\}$ has cardinality 2^{n-1}.*

From now on, we identify the vector space $\mathbf{F}_2^n$ with the finite field with 2^n elements, $\mathbf{F}_{2^n}$. Any function F from $\mathbf{F}_2^n$ into $\mathbf{F}_2^n$ can then be expressed as a polynomial in $\mathbf{F}_{2^n}[x]$. Recall that the *degree* of F is the maximal Hamming weight of its exponents:

$$\deg\left(\sum_{i=0}^{2^n-1} \lambda_i x^i\right) = \max\ \{\ wt(i) \mid \lambda_i \neq 0\ \},$$

where $\lambda_i \in \mathbf{F}_{2^n}$ and the weight is calculated on the 2-ary expansion of i. We denote by Tr the trace function on $\mathbf{F}_{2^n}$, i.e., $\mathrm{Tr}(\beta) = \beta + \beta^2 + \cdots + \beta^{2^{n-1}}$.

The function F can also be represented by n Boolean functions of n variables, its Boolean *coordinates*. Note that the coordinates are sometimes called the components of F, but it is more convenient for our purpose to use the following definition, like in [24].

Definition 3 *Let F be a function from $\mathbf{F}_{2^n}$ into $\mathbf{F}_{2^n}$. The linear combinations of the coordinates of F are the Boolean functions*

$$f_\lambda : x \in \mathbf{F}_{2^n} \mapsto \mathrm{Tr}(\lambda F(x)),\ \lambda \in \mathbf{F}_{2^n},$$

where f_0 is the null function. The functions f_λ are called the components *of F.*

We denote by $\mathcal{B}_n$ the set of Boolean functions on $\mathbf{F}_{2^n}$. In our context, the linear functions of $\mathcal{B}_n$ are the functions φ_a, defined by

$$\varphi_a : x \in \mathbf{F}_{2^n} \mapsto \mathrm{Tr}(ax)\ , a \in \mathbf{F}_{2^n}^*. \tag{1}$$

The following notation will be extensively used in the paper. For any $f \in \mathcal{B}_n$, we denote by $\mathcal{F}(f)$ the following value related to the Fourier (or Walsh) transform of f:

$$\mathcal{F}(f) = \sum_{x \in \mathbf{F}_{2^n}} (-1)^{f(x)} = 2^n - 2wt(f)\ , \tag{2}$$

where $wt(f)$ is the Hamming weight of f, i.e., the number of $x \in \mathbf{F}_2^n$ such that $f(x) = 1$. The function f is said to be *balanced* if and only if $\mathcal{F}(f) = 0$ or, equivalently, $wt(f) = 2^{n-1}$.

Definition 4 *The* Walsh spectrum *of $f \in \mathcal{B}_n$ is the multiset*[1]

$$\{\mathcal{F}(f + \varphi_a), a \in \mathbf{F}_{2^n}\}\ .$$

The nonlinearity *of f is its Hamming distance to the set of all affine functions. It is given by*

$$2^{n-1} - \frac{1}{2}\mathcal{L}(f) \quad \textit{where} \quad \mathcal{L}(f) = \max_{a \in \mathbf{F}_{2^n}} |\mathcal{F}(f + \varphi_a)|\ .$$

The lowest possible value for $\mathcal{L}(f)$ is $2^{\frac{n}{2}}$ and this bound is achieved for *bent functions.*

Definition 5 *[28, 6] Let $f \in \mathcal{B}_n$. The function f is said to be* plateaued *if its Walsh coefficients take at most three values, namely $0, \pm\mathcal{L}(f)$. Then, $\mathcal{L}(f) = 2^s$ with $s \geq n/2$.*

If $s = n/2$ (and n even) then f is said to be bent *and its Walsh coefficients take two values only, namely $\pm 2^{\frac{n}{2}}$. Moreover, f is said* plateaued optimal *if $s = (n+1)/2$ for odd n and $s = (n+2)/2$ for even n.*

These functions belong to a particular class of Boolean functions, which notably includes all quadratic functions and, more generally, *partially bent* [2] functions.

The nonlinearity of a function F from $\mathbf{F}_{2^n}$ into $\mathbf{F}_{2^n}$ is now defined by means of the nonlinearities of its components.

[1] A multiset is a set with repetition allowed. Thus the Walsh spectrum includes each value with the number of times it occurs.

[2] These functions were introduced in [10]; they can be seen as a generalization of quadratic functions.

Definition 6 *Let F be a function from $\mathbf{F}_{2^n}$ into $\mathbf{F}_{2^n}$ with components f_λ, $\lambda \in \mathbf{F}_{2^n}^*$. The* nonlinearity *of F is the minimal value of the nonlinearities of the f_λ. It is equal to*

$$\mathcal{N}(F) = 2^{n-1} - \frac{\Lambda(F)}{2} \text{ where } \Lambda(F) = \max_{\lambda \in \mathbf{F}_{2^n}^*} \mathcal{L}(f_\lambda).$$

The nonlinearity of F is a measure of its vulnerability to linear attacks. The functions that have maximal nonlinearity are called AB functions. They exist for odd n only.

Definition 7 *[13] Let F be a function from $\mathbf{F}_{2^n}$ into $\mathbf{F}_{2^n}$ with components f_λ, $\lambda \in \mathbf{F}_{2^n}$. Then,*

$$\Lambda(F) \geq 2^{\frac{n+1}{2}} \ .$$

The functions F which satisfy

$$\Lambda(F) = 2^{\frac{n+1}{2}}$$

are said to be almost bent (AB). *They exist when n is odd only. Moreover, if F is almost bent, then for any $a \in \mathbf{F}_{2^n}$ and for any nonzero λ*

$$\{\mathcal{F}(f_\lambda + \varphi_a),\ \lambda \in \mathbf{F}_{2^n}^*, a \in \mathbf{F}_{2^n}\} = \{0, \pm 2^{\frac{n+1}{2}}\}, \tag{3}$$

i.e., all f_λ, $\lambda \neq 0$, are plateaued optimal.

Remark 1 Let F be a function from $\mathbf{F}_{2^n}$ into $\mathbf{F}_{2^n}$. Studying the APN property and the AB property (for odd n) is equivalent to studying the weights of an associated code C_F and of its dual $C_F^\perp$ (see an extensive study in [11]).

The Walsh spectrum of a Boolean function and its derivatives are related by the so-called *sum-of-square indicator* introduced in [28] and extensively studied in [6, 7] and [29]. The proof of the following theorem can be found in [6] and [29].

Definition 8 *The* sum-of-square indicator *of $f \in \mathcal{B}_n$ is defined by:*

$$\nu(f) = \sum_{a \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_a f) = 2^{-n} \sum_{a \in \mathbf{F}_{2^n}} \mathcal{F}^4(f + \varphi_a) \ .$$

Theorem 1 *Any $f \in \mathcal{B}_n$ satisfies $\nu(f) \leq 2^n \mathcal{L}^2(f)$. Equality occurs if and only if f is plateaued, that is*

$$\mathcal{L}(f) = 2^s \quad \text{and} \quad \nu(f) = 2^{n+2s}, \quad \frac{n}{2} \leq s \leq n. \tag{4}$$

3 On APN functions

A necessary condition for a function F over $\mathbf{F}_{2^n}$ to be APN was provided by Nyberg in [24]. This condition involves the derivatives of the components of F. In this section, we prove that this condition is also a sufficient condition and derive another characterization by means of the sum-of-square indicators of the components of F. We further discuss some conjectures. We notably apply our characterization to achieve some new results on plateaued functions.

3.1 Characterizations of APN functions

The next theorem is mainly due to Nyberg [24]. We complete it only, providing a full characterization of APN functions by means of the derivatives of their component functions.

Theorem 2 *Let F be a function from $\mathbf{F}_{2^n}$ into $\mathbf{F}_{2^n}$ and let f_λ, $\lambda \in \mathbf{F}_{2^n}$ denote its components. Then, for any nonzero $a \in \mathbf{F}_{2^n}$:*

$$\sum_{\lambda \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) \geq 2^{2n+1}. \tag{5}$$

Moreover, F is APN if and only if for all nonzero $a \in \mathbf{F}_{2^n}$:

$$\sum_{\lambda \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = 2^{2n+1}. \tag{6}$$

Proof. We have :

$$\begin{aligned}
\sum_{\lambda \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) &= \sum_{\lambda, x, y \in \mathbf{F}_{2^n}} (-1)^{\mathrm{Tr}(\lambda(F(x+a)+F(x)+F(y+a)+F(y)))} \\
&= 2^n \#\{ (x,y) \in \mathbf{F}_{2^n}^2 \mid F(x+a)+F(x) = F(y+a)+F(y) \} \\
&= 2^{2n+1} + 2^n \#\{ (x,y) \mid D_a F(x) = D_a F(y),\ x \neq y \text{ and } y \neq x+a \}
\end{aligned}$$

Thus (5) is immediately deduced with equality if and only if F is APN (see Definition 2). $\diamond$

The previous theorem is more efficient for proving that F is not APN. For instance, if F is such that $D_a f_\lambda$ and $D_a f_{\lambda'}$ are constant, for $\lambda \neq \lambda' \neq 0$ and for some a, then the sum in (6) equals at least 2^{2n+2} ; so F is not APN. This argument was widely used for proving more general results [24]. Conversely, the sufficient condition induced by Theorem 2 leads to a better understanding of the properties of APN functions, as indicated in the next example.

Example 1 Let F be a polynomial of degree 3 on $\mathbf{F}_{2^n}$, where n is even. Thus, any component of F has degree at most 3. Any component f_λ, $\lambda \neq 0$, has all its derivatives of degree at most 2 (f_0 is the null function). This implies that for all λ and for all a, we have

$$\mathcal{F}(D_a f_\lambda) \equiv 0 \pmod{2^{(n+2)/2}},$$

a congruence which is satisfied by any quadratic non-bent function. Suppose that for any a, $|\mathcal{F}(D_a f_\lambda)|$ equals $2^{(n+2)/2}$ for exactly 2^{n-2} values of λ and equals 0 for the others. Then, by applying Theorem 2, F is APN. Is it possible to construct such a function F?

It follows from the previous theorem that the APN property is related to the values of the sum-of-square indicators, $\nu(f_\lambda)$, of the components of F.

Corollary 1 *Let F be a function from $\mathbf{F}_{2^n}$ into $\mathbf{F}_{2^n}$ with components f_λ, $\lambda \in \mathbf{F}_{2^n}^*$. Then*

$$\sum_{\lambda \in \mathbf{F}_{2^n}^*} \nu(f_\lambda) \geq (2^n - 1)2^{2n+1} \ . \tag{7}$$

Moreover, F is APN if and only if

$$\sum_{\lambda \in \mathbf{F}_{2^n}^*} \nu(f_\lambda) = (2^n - 1)2^{2n+1} \ . \tag{8}$$

Consequently, if $\nu(f_\lambda) = 2^{2n+1}$ for all nonzero λ, then F is APN.

Proof. Set $A = \sum_{a \in \mathbf{F}_{2^n}^*} \sum_{\lambda \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda)$. According to (5), we have $A \geq 2^{2n+1}(2^n - 1)$. Since $\mathcal{F}^2(D_0 f_\lambda) = \mathcal{F}^2(D_a f_0) = 2^{2n}$ for any a and for any λ, then

$$\sum_{a \in \mathbf{F}_{2^n}^*} \sum_{\lambda \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = \sum_{\lambda \in \mathbf{F}_{2^n}^*} \sum_{a \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = \sum_{\lambda \in \mathbf{F}_{2^n}^*} \nu(f_\lambda).$$

Thus $A = \sum_{\lambda \in \mathbf{F}_{2^n}^*} \nu(f_\lambda)$, implying (7). Now, if F is APN then F satisfies (6) and we get $A = 2^{2n+1}(2^n - 1)$. Conversely, assume that $A = 2^{2n+1}(2^n - 1)$. Since for any a

$$\sum_{\lambda \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) \geq 2^{2n+1},$$

these inequalities must be equalities. Then F is APN. The last statement is immediately deduced. ◇

Example 2 *When F is the inverse function $x \mapsto x^{2^n-2}$ over $\mathbf{F}_{2^n}$, it is well-known that F is APN for odd n et not APN for even n. The $\nu(f_\lambda)$ are calculated in [14]. As an illustration of our purpose we recall these values:*

- *Let n be odd. Thus $\Lambda(F) = \max \ \{ \ k \equiv 0 \pmod 4 \mid k < 2^{(n/2)+1} \ \}$ and, for all $\lambda \neq 0$, $\nu(f_\lambda) = 2^{2n+1}$.*
- *Let n be even. Thus $\Lambda(F) = 2^{(n+2)/2}$ and, for all $\lambda \neq 0$, $\nu(f_\lambda) = 2^{2n+1} + 2^{n+3}$.*

It appears from Corollary 1 that the APN property only depends on the extended Walsh spectrum of F, i.e., on the multiset

$$\mathcal{W}(F) = \{|\mathcal{F}(f_\lambda + \varphi_a)|, \ \lambda \in \mathbf{F}_{2^n}^*, \ a \in \mathbf{F}_{2^n}\} \ .$$

Note that $\mathcal{W}(F)$ consists of all values taken by $|\mathcal{F}(f_\lambda + \varphi_a)|$ and the number of times they occur. In other words, if F is APN, any function F' such that $\mathcal{W}(F') = \mathcal{W}(F)$ is APN too. Indeed, F is APN if and only if the $\nu(f_\lambda)$ satisfy (8). But the values $\nu(f_\lambda)$ are obtained by means of the values of the set $\mathcal{W}(F)$ (see Definition 8).

There are only a few extended Walsh spectra which are known to correspond to APN functions. When n is odd, three APN extended Walsh spectra are known

- $\mathcal{W}(x^3)$ whose elements lie in $\{0, 2^{\frac{n+1}{2}}\}$. It is the Walsh spectrum of all AB function;
- $\mathcal{W}(x^{2^n-2})$ whose elements take all values $k \equiv 0 \bmod 4$ such that $0 \leq k < 2^{\frac{n}{2}+1}$;
- $\mathcal{W}(x^{2^{4g}+2^{3g}+2^{2g}+2^g-1})$ for $n = 5g$ [16], which differs from both previous spectra since it contains a value which is not divisible by 2^{2g+1}, but all its elements are divisible by 4 (see Prop. 5.3 and 7.13 in [9]). For instance, for $n = 15$ (i.e., for $g = 3$), the values in $\mathcal{W}(x^{2^{4g}+2^{3g}+2^{2g}+2^g-1})$ are $0, 2^{2g}, 3 \cdot 2^{2g}, 2^{2g+2}, 5 \cdot 2^{2g}, 9 \cdot 2^{2g}$.

When n is even, only two APN extended Walsh spectra are known:

- $\mathcal{W}(x^3)$ whose elements lie in $\{0, 2^{\frac{n}{2}}, 2^{\frac{n}{2}+1}\}$.
- $\mathcal{W}(x^{2^{4g}+2^{3g}+2^{2g}+2^g-1})$ for $n = 5g$ [16], which differs from the previous one because it does not have the same divisibility as previously mentioned.

It is worth noticing that two functions F and G with different Walsh spectra may nevertheless be such that their components have the same sum-of-square indicators. For instance, when n is odd, all known APN functions on $\mathbf{F}_{2^n}$ are such that their components f_λ satisfy $\nu(f_\lambda) = 2^{2n+1}$ for all $\lambda \neq 0$. Conversely, two functions with the same extended Walsh spectrum may be such that the sets $\{\nu(f_\lambda),\ \lambda \in \mathbf{F}_{2^n}^*\}$ and $\{\nu(g_\lambda),\ \lambda \in \mathbf{F}_{2^n}^*\}$ are different, as we will see in Example 4.

Open Problem 1 *Find an APN function on $\mathbf{F}_{2^n}$, n odd, such that $\nu(f_\lambda) \neq 2^{2n+1}$ for some nonzero $\lambda \in \mathbf{F}_{2^n}^*$.*

Corollary 1 enables us to characterize APN functions when the corresponding sum-of-square indicators $\nu(f_\lambda)$ take their values in a particular set. Such a situation occurs for instance when all the $f_\lambda, \lambda \neq 0$, are plateaued functions, as pointed out in Corollaries 2 and 3. When n is odd, the situation is well-known. To be clear, we summarize it in the next corollary and give as proof a short explanation. The even case, which we treat in Corollary 3, is more interesting since we generalize the result of Nyberg [24, Theorem 10].

Corollary 2 *Let n be odd and let F be a function from $\mathbf{F}_{2^n}$ into $\mathbf{F}_{2^n}$ with components f_λ, $\lambda \in \mathbf{F}_{2^n}^*$. Then, the following statements are equivalent:*

(i) *F is APN and all f_λ, $\lambda \in \mathbf{F}_{2^n}^*$ are plateaued;*

(ii) *all f_λ, $\lambda \in \mathbf{F}_{2^n}^*$, are plateaued and satisfy $\nu(f_\lambda) = 2^{2n+1}$;*

(iii) *F is AB.*

Proof. If f_λ is plateaued, then we have $\nu(f_\lambda) = 2^{n+2s}$ with $2s \geq n+1$ (see Theorem 1). If F is APN, then Relation (8) is satisfied with $\nu(f_\lambda) \geq 2^{2n+1}$ for all λ, implying **(ii)**. We deduce from Corollary 1 that **(ii)** implies that F is APN. The equivalence between **(ii)** and **(iii)** is mentioned in Definition 7. ◇

Corollary 3 *Let n be even and let F be a function from $\mathbf{F}_{2^n}$ into $\mathbf{F}_{2^n}$ such that all f_λ, $\lambda \in \mathbf{F}_{2^n}^*$, are plateaued. Let B be the number of f_λ which are bent. Then we have:*

(i) *If $B = 0$ then F is not APN;*

(ii) *If F is APN, then $B \geq 2 \cdot (2^n - 1)/3$ with equality if and only if $\Lambda(F) = 2^{(n+2)/2}$. Conversely, if $B = 2 \cdot (2^n - 1)/3$ and $\Lambda(F) = 2^{(n+2)/2}$ then F is APN.*

(iii) *If F is APN then it is not a permutation. Moreover, there is no permutation of the form $F + L$ where L is a linear function on $\mathbf{F}_{2^n}$.*

Proof.

(i) Assume that there is no $\lambda \neq 0$ such that f_λ is bent. Since n is even, we then have $\nu(f_\lambda) \geq 2^{2n+2}$ for all λ which contradicts (8). Thus F is not APN.

(ii) Suppose now that F is APN. Thus (8) holds implying that for some λ we must have $\nu(f_\lambda) = 2^{2n}$, *i.e.* f_λ is bent. More precisely:

$$\sum_{\lambda \in \mathbf{F}_{2^n}^*} \nu(f_\lambda) = (2^n - 1)2^{2n+1} = B2^{2n} + N2^{2n+2}$$

and $B + N \geq 2^n - 1$. We must have $B = 2(2^n - 1) - 4N$ with $-N \leq B - (2^n - 1)$. Hence $B \leq 4B - 2(2^n - 1)$ which leads to $B \geq 2 \cdot (2^n - 1)/3$ with equality if and only if $N = (2^n - 1)/3$. It is equivalent to saying that any non bent component f_λ satisfies $\nu(f_\lambda) = 2^{2n+2}$ and $\mathcal{L}(f_\lambda) = 2^{(n+2)/2}$ (since it is plateaued). It implies that $\Lambda(F) = 2^{(n+2)/2}$. Conversely, assume that $B = 2 \cdot (2^n - 1)/3$ and $\Lambda(F) = 2^{(n+2)/2}$. Thus, the $(2^n - 1)/3$ non bent components satisfies $\nu(f_\lambda) = 2^{2n+2}$ and (8) holds.

(iii) The functions f_λ which are bent cannot be balanced. If F is APN then there exists λ such that f_λ is bent. Thus, F cannot be a permutation. Moreover, for any linear function L, the component $(F+L)_\lambda$ is equal to $f_\lambda + \varphi$ for some linear Boolean function φ. Therefore, it is bent, implying that $F + L$ is not a permutation.

◇

Example 3 There exist APN functions as characterized in the previous corollary. The most famous one is $F : x \mapsto x^3$ where f_λ is bent if and only if $\lambda \neq a^3$ for all $a \in \mathbf{F}_{2^n}$. Note that $x \mapsto x^3$ is APN for any n; it is AB for odd n.

Example 4 Let us consider an APN function F on $\mathbf{F}_{2^n}$ such that all its components f_λ, $\lambda \in \mathbf{F}_{2^n}^*$, are plateaued. When n is odd, Corollary 2 implies that, for any function G which has the same extended Walsh spectrum as F, all components g_λ, $\lambda \in \mathbf{F}_{2^n}^*$, are plateaued optimal. For instance, the function

$$G : x \mapsto x^{2^i+1} + (x^{2^i} + x)\mathrm{Tr}(x^{2^i+1} + x),\ 1 \leq i < \frac{n+1}{2}, \gcd(i, n) = 1$$

defined in [5] is CCZ-equivalent to $x \mapsto x^{2^i+1}$. Therefore, G is AB, implying that, for any $\lambda \neq 0$, we have $\nu(g_\lambda) = 2^{2n+1}$.

When n is even, the situation is completely different. For instance, the APN function defined in [5]:

$$G : x \mapsto x^{2^i+1} + (x^{2^i} + x + 1)\mathrm{Tr}(x^{2^i+1}),\ 1 \leq i < \frac{n}{2}, \gcd(i,n) = 1$$

has the same Walsh spectrum as x^3. But, it does not imply that all its components are plateaued. For instance, for $n = 6$ and $i = 1$, $\nu(g_\lambda)$, $\lambda \neq 0$, takes 30 times the value 2^{12}, 24 times the value $2^{13} + 2^{11}$ and 9 times the value 2^{14}. Obviously, the g_λ for which $\nu(g_\lambda) = 2^{13} + 2^{11}$ are not plateaued.

The previous example points out that the APN property may lead to different sets $\{\nu(f_\lambda), \lambda \in \mathbf{F}_{2^n}^*\}$ whereas only one configuration is known in the odd case. A natural question is to determine whether the configuration that appears in the odd case may also occur when n is even.

Open Problem 2 *Does there exist an APN function F of $\mathbf{F}_{2^n}$, n even, such that $\nu(f_\lambda) = 2^{2n+1}$ for all $\lambda \in \mathbf{F}_{2^n}^*$?*

3.2 APN permutations

The existence of APN permutations of an even number of variables is a major open problem, especially for the design of block ciphers since practical cryptosystems act on an even number of variables due to implementation constraints. In this subsection, we discuss this open problem.

Open Problem 3 *Let F be a permutation on $\mathbf{F}_{2^n}$, n even. Is it possible for F to be APN?*

We will first review what is known about this problem.

Theorem 3 *Let F be any permutation on $\mathbf{F}_{2^n}$, $n = 2t$.*

(o) *If $n = 4$ then F cannot be APN.*

(i) *If $F \in \mathbf{F}_4[x]$ then F is not APN.*

(ii) *If $F \in \mathbf{F}_{2^t}[x]$ then F is not APN.*

(iii) *If F is such that all its components f_λ, $\lambda \in \mathbf{F}_{2^n}^*$, are plateaued then F cannot be APN.*

Proof. **(o)** was proved using a computer, for instance in [20]. **(i)** is easy to prove, since if $F \in \mathbf{F}_4[x]$ then $F(\mathbf{F}_4) = \mathbf{F}_4$. Thus, with $\mathbf{F}_4 = \{0, 1, \beta, \beta + 1\}$, we obtain:

$$F(0) + F(1) + F(\beta) + F(\beta + 1) = 0.$$

(ii) was proved by Hou [20].

The following result was proved by Nyberg in [23]: *Let n be even. If any permutation F is such that all its components f_λ, $\lambda \in \mathbf{F}_{2^n}^*$, are partially bent then F cannot be APN; in particular there is no quadratic APN permutation of $\mathbf{F}_{2^n}$.* Partially bent functions are a kind of plateaued functions which have linear structures and the proof of Nyberg fruitfully used the necessary condition given by Theorem 2. Our Corollary 3 generalizes this result, proving **(iii)**.

◇

Now, we show that APN permutations are completely characterized by the derivatives of their components. Recall that F is a permutation on $\mathbf{F}_{2^n}$ if and only if all its components f_λ, $\lambda \in \mathbf{F}_{2^n}^*$ are balanced. It is well-known that this is equivalent to

$$\sum_{a \in \mathbf{F}_{2^n}^*} \mathcal{F}(D_a f_\lambda) = -2^n, \quad \forall\, \lambda \in \mathbf{F}_{2^n}^*. \tag{9}$$

We can also use another characterization which leads to the following result.

Proposition 2 *Let F be a function from $\mathbf{F}_{2^n}$ into $\mathbf{F}_{2^n}$ with components f_λ, $\lambda \in \mathbf{F}_{2^n}^*$. Then F is a permutation if and only if, for all $a \in \mathbf{F}_{2^n}^*$, we have*

$$\sum_{\lambda \in \mathbf{F}_{2^n}^*} \mathcal{F}(D_a f_\lambda) = -2^n$$

Consequently F is an APN permutation if and only if, for any $a \in \mathbf{F}_{2^n}^*$,

$$\sum_{\lambda \in \mathbf{F}_{2^n}^*} \mathcal{F}(D_a f_\lambda) = -2^n \text{ and } \sum_{\lambda \in \mathbf{F}_{2^n}^*} \mathcal{F}^2(D_a f_\lambda) = 2^{2n}\ .$$

Proof.

$$\begin{aligned} \sum_{\lambda \in \mathbf{F}_{2^n}^*} \mathcal{F}(D_a f_\lambda) &= \sum_{\lambda \in \mathbf{F}_{2^n}^*} \sum_{x \in \mathbf{F}_{2^n}} (-1)^{\mathrm{Tr}(\lambda(F(x)+F(x+a)))} \\ &= \sum_{x \in \mathbf{F}_{2^n}} \sum_{\lambda \in \mathbf{F}_{2^n}^*} (-1)^{\mathrm{Tr}(\lambda(F(x)+F(x+a)))}. \end{aligned}$$

The last sum is clearly equal to -2^n if and only if $F(x) + F(x+a) \neq 0$ for all x and for all $a \neq 0$. This means that F is a permutation. The last statement of the proposition is oviously deduced, by using Theorem 2. ◇

3.3 APN power functions

More results on the APN property are known when we focus on the family of power functions, *i.e.*, $F : x \mapsto x^d$ over $\mathbf{F}_{2^n}$. For instance, *if there is h which divides n and $d = k(2^h - 1) + 2^r$ for some k and r then F is not APN* [15, 11]. Also if F is APN then $gcd(d, 2^n - 1)$ is known. We present this last result, indicated by Hans Dobbertin, in a more general context.

Proposition 3 *Let r be a divisor of n. Let F be any function on $\mathbf{F}_{2^n}$. Assume that $F \in \mathbf{F}_{2^r}[x]$. If F satisfies for some $a \in \mathbf{F}_{2^r}$:*

$$F(y) + F(y+a) = \beta \ , \quad \beta \in \mathbf{F}_{2^r},$$

for some y such that $y \notin \mathbf{F}_{2^r}$ and $y^{2^r} + y + a \neq 0$, then F is not APN.

Consequently, if F is APN with $F(x) = x^d$, then $gcd(d, 2^n - 1) = 1$ for odd n and $gcd(d, 2^n - 1) = 3$ for even n.

Proof. Since F lies in $\mathbf{F}_{2^r}[x]$ then the polynomial $G(x) = F(x) + F(x+a)$ is in $\mathbf{F}_{2^r}[x]$ too. Let $y \notin \mathbf{F}_{2^r}$ such that the hypotheses are satisfied. Thus

$$(G(y))^{2^r} = \beta = F(y^{2^r}) + F(y^{2^r} + a) = F(y) + F(y+a)$$

where $y^{2^r} \notin \{y, y+a\}$. According to Definition 2, F cannot be APN.

Let $F(x) = x^d$ and set $s = gcd(d, 2^n - 1)$. Note that such a polynomial F is in $\mathbf{F}_2[x]$. Notably, it cannot be an APN permutation for even n. Assume that $s > 1$. Hence there is $y \notin \mathbf{F}_2$ such that $y^d = 1$. Observe that $x \mapsto (x+1)/x$ is a bijection on $\mathbf{F}_{2^n} \setminus \{0, 1\}$ and set $y = (z+1)/z$. Then we get

$$\frac{(z+1)^d}{z^d} = 1 \ , \ i.e. \ (z+1)^d + z^d = 0.$$

So, we have $z \notin \mathbf{F}_2$ such that $F(z) + F(z+1) = 0$. When n is odd, it is impossible to have $z^2 + z + 1 = 0$. So, if F is APN, the hypothesis $s > 1$ leads to a contradiction (according to the first part of the proposition). We then conclude that $s = 1$ for odd n.

Assume now that n is even and F is APN. This is possible only if $z^2 + z + 1 = 0$, that is $z \in \mathbf{F}_4$ (so $y \in \mathbf{F}_4$). Then, in this case, $y^d = 1$ implies $y \in \mathbf{F}_4$. We conclude that $s = 3$, since $s > 3$ would lead to a contradiction ($y^d = 1$ for a subgroup larger than $\mathbf{F}_4^*$). This completes the proof. ◇

The fact that, for power functions, the APN property has a deeper relationship with the Walsh spectrum of the function is due to the following result.

Proposition 4 *Let F be any function on $\mathbf{F}_{2^n}$ of the form $x \mapsto x^d$. Let f_λ denote the components of F. Set $s = \gcd(d, 2^n - 1)$ and $2^n - 1 = us$. Let α be a primitive element of $\mathbf{F}_{2^n}$. Then $\mathcal{F}(D_a f_\lambda) = \mathcal{F}(D_1 f_{\lambda a^d})$ for all $a, \lambda \in \mathbf{F}_{2^n}^*$.*

Moreover,

$$\nu(f_\lambda) = 2^{2n} + s \sum_{i=0}^{u-1} \mathcal{F}^2(D_1 f_{\lambda \alpha^{id}}).$$

and

$$\sum_{\lambda \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = \frac{1}{s} \sum_{j=0}^{s-1} \nu(f_{\alpha^j}) \ .$$

Proof. We have, for any nonzero a:

$$\begin{aligned}\mathcal{F}(D_a f_\lambda) &= \sum_{x\in\mathbf{F}_{2^n}} (-1)^{\mathrm{Tr}(\lambda(x^d+(x+a)^d))} \\ &= \sum_{x\in\mathbf{F}_{2^n}} (-1)^{\mathrm{Tr}(\lambda a^d((\frac{x}{a})^d+(\frac{x}{a}+1)^d))} \\ &= \sum_{y\in\mathbf{F}_{2^n}} (-1)^{\mathrm{Tr}(\lambda a^d(y^d+(y+1)^d))} = \mathcal{F}(D_1 f_{\lambda a^d}),\end{aligned}$$

by replacing $y = x/a$. Now,

$$\begin{aligned}\nu(f_\lambda) &= \sum_{a\in\mathbf{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) \\ &= 2^{2n} + \sum_{i=0}^{2^n-2} \mathcal{F}^2(D_1 f_{\lambda\alpha^{id}}) \\ &= 2^{2n} + s\sum_{i=0}^{u-1} \mathcal{F}^2(D_1 f_{\lambda\alpha^{id}}) \\ &= 2^{2n} + s\sum_{i=0}^{u-1} \mathcal{F}^2(D_1 f_{\lambda\alpha^{is}}) \qquad (10)\end{aligned}$$

since $\alpha^{vud} = 1$ for $1 \le v \le s-1$. Moreover, for any $a \in \mathbf{F}_{2^n}^*$, we have

$$\begin{aligned}\sum_{\lambda\in\mathbf{F}_{2^n}^*} \mathcal{F}^2(D_a f_\lambda) &= \sum_{\lambda\in\mathbf{F}_{2^n}^*} \mathcal{F}^2(D_1 f_{\lambda a^d}) \\ &= \sum_{i=0}^{s-1}\sum_{j=0}^{u-1} \mathcal{F}^2(D_1 f_{\alpha^i\alpha^{js}}) \ ,\end{aligned}$$

where the last equation is obtained by writing $\lambda = \alpha^{i+js}$ and $a^d = \alpha^{ks}$. We then deduce from (10) that

$$\sum_{\lambda\in\mathbf{F}_{2^n}^*} \mathcal{F}^2(D_a f_\lambda) = \frac{1}{s}\sum_{j=0}^{s-1} \left(\nu(f_{\alpha^j}) - 2^{2n}\right) \ .$$

The result now comes from the fact that $\mathcal{F}^2(D_a f_\lambda) = 2^{2n}$ for $\lambda = 0$. ◇

Now, the situation when n is odd is quite clear as pointed out in the following proposition. Note that this proposition includes all APN power functions since any APN power function is a permutation when n is odd.

Proposition 5 *Let F be any function on $\mathbf{F}_{2^n}$ of the form $x \mapsto x^d$. Let f_λ denote the components of F. Assume that* $\gcd(d, 2^n - 1) = 1$. *Then the $\nu(f_\lambda)$, $\lambda \in \mathbf{F}_{2^n}^*$, are equal and*

$$\nu(f_1) = \sum_{\lambda \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_1 f_\lambda).$$

Moreover these statements, which are possible for odd n only, are equivalent:

(i) *F is an APN permutation;*

(ii) *$\nu(f_\lambda) = 2^{2n+1}$ for some λ;*

(iii) $\sum_{\lambda \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_1 f_\lambda) = 2^{2n+1}$.

Proof. According to the previous proposition, we have for any λ:

$$\nu(f_\lambda) = 2^{2n} + \sum_{i=0}^{2^n-2} \mathcal{F}^2(D_1 f_{\lambda \alpha^{id}}) = \sum_{\mu \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_1 f_\mu),$$

since $s = 1$ and $x \mapsto x^d$ is a permutation on $\mathbf{F}_{2^n}$. The second statement is directly deduced from Theorem 2. Recall that F cannot be APN for even n (see Theorem 3,**(iii)**). ◇

The fact that F APN, with $F(x) = x^d$ over $\mathbf{F}_{2^n}$ (n odd), implies that $\nu(\mathrm{Tr}(x^d)) = 2^{2n+1}$ when $\gcd(d, 2^n - 1) = 1$, was proved by Helleseth [18] in another context (see also [8]).

Here again, the situation is very different when n is even as pointed out in the following theorem. Recall that $\Lambda(F)$ is defined by Definition 6. Note that it is conjectured that $\Lambda(F)$ cannot be less than $2^{(n+2)/2}$ for even n. We prove here that this is true for APN power functions.

Theorem 4 *Let $n = 2t$ be an even integer and let F be any function on $\mathbf{F}_{2^n}$ of the form $x \mapsto x^d$. Let f_λ denote the components of F. Then, F is APN if and only if*

$$\nu(f_1) + 2\nu(f_\alpha) = 3 \cdot 2^{2n+1}$$

where α is a primitive element of $\mathbf{F}_{2^n}$.

Moreover, if F is APN, then it satisfies

$$\mathcal{F}(f_\lambda) = \begin{cases} (-1)^{t+1} 2^{t+1} & \text{if } \lambda \in \{x^3,\ x \in \mathbf{F}_{2^n}^*\} \\ (-1)^t 2^t & \text{if } \lambda \notin \{x^3,\ x \in \mathbf{F}_{2^n}^*\} \end{cases},$$

implying that

$$\Lambda(F) \geq 2^{t+1},$$

i.e., *the nonlinearity of such F satisfies $\mathcal{N}(F) \leq 2^{n-1} - 2^t$.*

Proof. Assume that $\gcd(d, 2^n - 1) = 3$. Thus, from Proposition 4, we have for any a:

$$3 \sum_{\lambda \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = \nu(f_1) + 2\nu(f_\alpha),$$

where α is a primitive element of $\mathbf{F}_{2^n}$. This comes from the fact that $\nu(f_\alpha) = \nu(f_{\alpha^2})$ because both functions are linearly equivalent.

Recall that if $F : x \mapsto x^d$ is APN, we have $\gcd(d, 2^n - 1) = 3$ (see Proposition 3). Hence, according to Theorem 2, F is APN if and only if

$$\nu(f_1) + 2\nu(f_\alpha) = 3 \cdot 2^{2n+1}.$$

Let g_λ, $\lambda \in \mathbf{F}_{2^n}$, denote the components of $G : x \mapsto x^3$ over $\mathbf{F}_{2^n}$. If $F : x \mapsto x^d$ is APN then $d = 3^r k$, $r > 0$, with $gcd(d, 2^n - 1) = 3$. Thus we have :

$$\begin{aligned} \mathcal{F}(f_\lambda) &= \sum_{x \in \mathbf{F}_{2^n}} (-1)^{\mathrm{Tr}(\lambda x^d)} \\ &= \sum_{y \in \mathbf{F}_{2^n}} (-1)^{\mathrm{Tr}(\lambda y^{3^r})} \\ &= \sum_{z \in \mathbf{F}_{2^n}} (-1)^{\mathrm{Tr}(\lambda z^3)} = \mathcal{F}(g_\lambda). \end{aligned}$$

This is because $x \mapsto x^d$ is 3-to-1 from $\mathbf{F}_{2^n}^*$ to the set $\{ z^3 \mid z \in \mathbf{F}_{2^n} \}$, since $u^d = v^d$ if and only if $(u/v)^3 = 1$, that is $u = v\beta$ where $\beta \in \mathbf{F}_4^*$.

Now we have $\mathcal{F}(f_\lambda) = \mathcal{F}(g_\lambda)$ with $g_\lambda(x) = \mathrm{Tr}(\lambda x^3)$. The values of $\mathcal{F}(g_\lambda)$ were determined by Carlitz [12, Theorem 1]:

$$\mathcal{F}(g_\lambda) = \begin{cases} (-1)^{t+1} 2^{t+1} \\ (-1)^t 2^t \end{cases},$$

according as λ is or is not a cube in $\mathbf{F}_{2^n}^*$. We deduce that

$$\mathcal{F}(f_1) = -2^{t+1} \text{ and } \mathcal{F}(f_\alpha) = 2^t \ ;$$

for even t and

$$\mathcal{F}(f_1) = 2^{t+1} \text{ and } \mathcal{F}(f_\alpha) = -2^t$$

for odd t. Moreover, we have for any t :

$$\Lambda(F) \geq |\mathcal{F}(f_1)| = 2^{t+1} \ .$$

◇

Recall that for odd n, it is well-known that $\Lambda(F) \geq 2^{(n+1)/2}$ for any function F on $\mathbf{F}_{2^n}$ whose image has dimension n. The next conjecture comes naturally from the previous result.

Conjecture 1 *Let F be any function on $\mathbf{F}_{2^n}$ where $n = 2t$. If F is APN then $\Lambda(F) \geq 2^{t+1}$.*

Example 5 For APN power functions over $\mathbf{F}_{2^n}$, n even, two different situations are known.

- For Gold exponents, $d = 2^i + 1$, $\gcd(i, n) = 1$, $1 \leq i < \frac{n}{2}$, we have

  $$\nu(f_1) = 2^{2n+2} \text{ and } \nu(f_\alpha) = 2^{2n} \ .$$

  This corresponds to the situation described in Corollary 3. These functions achieve the highest possible nonlinearity for an APN power function as shown in the previous theorem.

- For Dobbertin's exponent, $d = 2^{4g} + 2^{3g} + 2^{2g} + 2^g - 1$ when $n = 5g$, we have for $n \in \{10, 20\}$

  $$\nu(f_1) = 2^{2n+1} + 2^{n+2g+1}\left(2^{2g} + 2^g - 1\right) \text{ and } \nu(f_\alpha) = 2^{2n+1} - 2^{n+2g}\left(2^{2g} + 2^g - 1\right) \ .$$

  Here, we have $\Lambda(F) > 2^{\frac{n}{2}+1}$.

3.4 Functions with $\delta(\mathbf{F}) \geq 4$

We previously focused on APN functions, i.e., the functions for which $\delta(F) = 2$ with

$$\delta(F) = \max_{a \neq 0,\ b \in \mathbf{F}_2^n} \#\{x \in \mathbf{F}_2^n,\ D_a F(x) = b\}.$$

Now, we point out that some results on the sum-of-square indicators of the components of F can be derived from Nyberg's result [24], when $\delta(F) \geq 4$.

Proposition 6 *Let F be a function from $\mathbf{F}_{2^n}$ into $\mathbf{F}_{2^n}$ with components f_λ, $\lambda \in \mathbf{F}_{2^n}^*$. Then, there exists $a \in \mathbf{F}_{2^n}^*$ such that*

$$\sum_{\lambda \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) \geq 2^{2n+1} + 2^n \delta(F)(\delta(F) - 2) \ .$$

Proof. We use the same notation as in Definition 2. Let $a \in \mathbf{F}_{2^n}^*$ be such that there exists $b \in \mathbf{F}_{2^n}$ with $\delta(a, b) = \delta(F)$. Let A_i denote the number of $b \in \mathbf{F}_{2^n}$ such that $\delta(a, b) = i$. Recall the following formula due to Nyberg [24]: for any $a \in \mathbf{F}_{2^n}^*$

$$\sum_{\lambda \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = 2^n \sum_{b \in \mathbf{F}_{2^n}} \delta^2(a, b) \ .$$

We deduce that

$$\begin{aligned} 2^{-n} \sum_{\lambda \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) &= \delta(F)^2 A_{\delta(F)} + \sum_{i=2}^{\delta(F)-2} i^2 A_i \qquad (11) \\ &\geq \delta(F)^2 A_{\delta(F)} + 2 \sum_{i=2}^{\delta(F)-2} i A_i \ , \end{aligned}$$

with equality if and only if $\delta(a,b) \in \{\delta(F), 2, 0\}$ for all $b \in \mathbf{F}_{2^n}$. Moreover, we have

$$\sum_{i=2}^{\delta(F)-2} iA_i = 2^n - \delta(F)A_{\delta(F)} \ . \tag{12}$$

Thus,

$$\sum_{\lambda \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) \geq 2^{2n+1} + 2^n \delta(F)(\delta(F)-2) \ ,$$

with equality if and only if $A_{\delta(F)} = 1$ and $A_i = 0$ for all $4 \leq i \leq \delta(F) - 2$. ◇

Corollary 4 *Let F be a power permutation on $\mathbf{F}_{2^n}$, n even, i.e., $F(x) = x^d$ with $\gcd(d, 2^n - 1) = 1$. Let f_λ denote the components of f. Then, all $\nu(f_\lambda)$, $\lambda \in \mathbf{F}_{2^n}^*$, are equal and satisfy*

$$\nu(f_\lambda) \geq 2^{2n+1} + 2^{n+3} \ .$$

Moreover, if equality holds, then $\delta(F) = 4$.

Proof. When F is a power permutation, we have from Proposition 5 that, for all $\lambda \in \mathbf{F}_{2^n}^*$,

$$\nu(f_\lambda) = \sum_{\mu \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_1 f_\mu) \ .$$

Moreover, we know from Proposition 4 that, for any $a \in \mathbf{F}_{2^n}^*$,

$$\sum_{\mu \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_1 f_\mu) = \sum_{\mu \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_a f_\mu) \ .$$

From the previous proposition, we deduce that, for all $\lambda \in \mathbf{F}_{2^n}^*$,

$$\nu(f_\lambda) \geq 2^{2n+1} + 2^n \delta(F)\left(\delta(F) - 2\right) \ .$$

When n is even, F cannot be APN, i.e., $\delta(F) \geq 4$. Thus, it implies that

$$\nu(f_\lambda) \geq 2^{2n+1} + 2^{n+3} \text{ for all } \lambda \in \mathbf{F}_{2^n}^* \ . \tag{13}$$

Conversely, any power permutation which satisfies (13) with equality is such that $\delta(F) = 4$. Indeed, we clearly have that $\delta(F) \geq 4$ from Corollary 1. Moreover, for $\delta(F) \geq 6$, we would have

$$\nu(f_\lambda) \geq 2^{2n+1} + 3 \cdot 2^{n+3} \text{ for all } \lambda \in \mathbf{F}_{2^n}^* \ .$$

◇

Example 6 When n is even, the inverse function $F : x \mapsto x^{2^n-2}$ over $\mathbf{F}_{2^n}$, which is used in the AES S-boxes, satisfies

$$\nu(f_\lambda) = 2^{2n+1} + 2^{n+3} \text{ for all } \lambda \in \mathbf{F}_{2^n}^*$$

(see Example 2). Then, the sum-of-square indicators of its components achieve the lowest possible value for a power permutation of $\mathbf{F}_{2^n}$ when n is even.

Since it is still unknown whether APN permutations of $\mathbf{F}_{2^n}$ exist when n is even, the use of permutations F with $\delta(F) = 4$ is suitable in cryptographic applications. When F is not a power function, the values

$$\sum_{\lambda \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda)$$

may differ when a varies. We know from (11) and (12) that any function F with $\delta(F) = 4$ satisfies

$$\sum_{\lambda \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = 2^{2n+1} + 2^{n+3} A_4(a)$$

where $A_4(a)$ is the number of $b \in \mathbf{F}_{2^n}$ such that $\delta(a, b) = 4$. Therefore, we have

$$\sum_{\lambda \in \mathbf{F}_{2^n}^*} \nu(f_\lambda) = (2^n - 1)2^{2n+1} + A2^{n+3} \tag{14}$$

where $A = \sum_{a \in \mathbf{F}_{2^n}^*} A_4(a)$. Note that, if the sum-of-square indicators are such that (14) is satisfied for $A \in \{1, 2\}$, then $\delta(F) = 4$. Indeed, $\delta(F) = 2$ implies that

$$\sum_{\lambda \in \mathbf{F}_{2^n}^*} \nu(f_\lambda) = (2^n - 1)2^{2n+1} \ ,$$

from Corollary 1. Moreover, if $\delta(F) \geq 6$, we deduce from Proposition 6 and Theorem 2 that

$$\begin{aligned} \sum_{\lambda \in \mathbf{F}_{2^n}^*} \nu(f_\lambda) &= \sum_{a \in \mathbf{F}_{2^n}^*} \sum_{\lambda \in \mathbf{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) \\ &\geq (2^n - 1)2^{2n+1} + 3 \cdot 2^{n+3} \ . \end{aligned}$$

The case $A = 2^n - 1$ in (14) is achieved by the inverse function which is such that $A_4(a) = 1$ for any nonzero a. However, we can wonder whether some functions F with $\delta(F) = 4$ achieve a lower value for A. Thus, the following open problem arises.

Open Problem 4 *Find a permutation F on $\mathbf{F}_{2^n}$, n even, with components f_λ, $\lambda \in \mathbf{F}_{2^n}^*$, such that $\delta(F) = 4$ and*

$$\sum_{\lambda \in \mathbf{F}_{2^n}^*} \nu(f_\lambda) = (2^n - 1)2^{2n+1} + A2^{n+3}$$

for some integer $A < 2^n - 1$.

4 Quadratic APN functions

An infinite class of quadratic APN functions, which are not equivalent to any power function, was characterized very recently (see [4] and [17]). This disproves a conjecture on APN

functions of degree 2, saying that such functions are equivalent to the power functions $x \mapsto x^{2^k+1}$ over $\mathbf{F}_{2^n}$ with $\gcd(k,n) = 1$ and $1 \leq k \leq n/2$. Here, we contribute to the classification of APN quadratic functions. We prove that there are no APN quadratic functions on $\mathbf{F}_{2^n}$ of the form

$$F(x) = \sum_{i=1}^{n-1} c_i x^{2^i+1} \ , \quad c_i \in \mathbf{F}_{2^n}, \tag{15}$$

except the previously mentioned power functions. We will use the Hermite's criterion. A proof of the next theorem can be found in [22, Theorem 7.4].

Theorem 5 [Hermite's criterion] *Let $\mathbf{F}_q$ be any finite field of characteristic p. Then a polynomial $P \in \mathbf{F}_q[x]$ is a permutation polynomial of $\mathbf{F}_q$ if and only if both following conditions hold:*

(i) *P has exactly one root in $\mathbf{F}_q$;*

(ii) *for each integer t with $1 \leqslant t < q-1$ such that $t \not\equiv 0 \pmod p$, the degree of $P(x)^t \pmod{x^q - x}$ is less than or equal to $q-2$.*

In order to specify our purpose, we first discuss some open problems.

4.1 Some open problems

Let F be a quadratic function on $\mathbf{F}_{2^n}$. Then, for any a, the function D_aF is affine or constant. Thus, it is obviously deduced from Proposition 1:

Corollary 5 *Any quadratic function F on $\mathbf{F}_{2^n}$ is APN if and only if for all non zero a, the set $\{D_aF(x), x \in \mathbf{F}_2^n\}$ is a flat of codimension 1.*

Recall that when n is odd then any quadratic function F is APN if and only if it is AB, that is all coordinate functions of F are plateaued optimal. Note that we proved this property for non quadratic functions by Corollary 2.

More generally, Bending et al. introduced *crooked* functions in [1, 27]. Such a function F is defined on $\mathbf{F}_{2^n}$ with n odd and is such that for all non zero a, the set $\{D_aF(x), x \in \mathbf{F}_2^n\}$ is an affine hyperplane. Crooked functions are AB and the only known *crooked* functions are quadratic.

Open Problem 5 *Construct crooked functions which are not quadratic.*

Another problem is about the characterization of APN quadratic functions which are not affinely equivalent to a power function. Note that in [5], Budaghyan, Carlet and Pott exhibit the first known APN functions which are not affinely equivalent to a power function, but these are of degree greater than 2. The first class of APN quadratic functions, not equivalent to a power function, was recently exhibited in [4] and [17]. It is composed of binomials of Clearly, the classification of APN quadratic functions is not yet achieved. $\mathbf{F}_{2^n}[x]$ with $n = 3k$ and $gcd(3,k) = 1$.

Open Problem 6 *Find new classes of APN quadratic functions. Notably, prove that there are APN quadratic functions which are not equivalent to a power function for $n \neq 3k$, where $gcd(3,k) = 1$.*

In the next section, we prove that the class of quadratic functions defined by (15) is APN only when it is an APN power function. Notably, our next Theorem 6 has the following consequence.

Proposition 7 *Let F be any quadratic function which is not a power function. Then if F is APN its expression contains at least one term of the form $cx^{2^i+2^j}$, $c \in \mathbf{F}_{2^n}^*$, where $i > 0$ and $j > 0$.*

4.2 On a class of quadratic functions

Note that (15) is not the general expression of quadratic functions on $\mathbf{F}_{2^n}$ since it does not include any term of the form $x^{2^i+2^j}$, with $i, j > 0$. On the other hand, note that if F is APN then $F + L$ is APN too, where L is any affine polynomial. We first prove a useful lemma in order to characterize the APN property for the class of quadratic functions defined by (15).

Lemma 1 *Let H be a polynomial on $\mathbf{F}_{2^n}$ such that $H(0) = 0$ and satisfying:*

$$\forall\ a,\ \forall\ b,\ a \neq b \neq 0, \quad H(a) \neq H(b), \tag{16}$$

and $H(e) = 0$ for a unique $e \neq 0$. Then the degree of H is exactly $2^n - 1$.

Proof. Since $H(0) = H(e) = 0$, then H is not a permutation. The image of H, *i.e.*, the set $I = \{H(x) | x \in \mathbf{F}_{2^n}\}$, contains exactly $2^n - 1$ elements, including 0, which appears twice. Thus there is only one nonzero element, say $\beta \in \mathbf{F}_{2^n}^*$, which is not in I. Let us define the polynomial P on $\mathbf{F}_{2^n}$ by

$$P(x) \ = \ \begin{cases} H(x) & \text{for } x \neq e \\ \beta & \text{for } x = e \end{cases} .$$

Then the image of P has cardinality 2^n, meaning that P is a permutation. Now we are going to express the polynomial $W = H + P$. Note that, from the definition of P, $W(x) = 0$ unless $x = e$ and $W(e) = P(e) = \beta$. We claim that the unique representation of W modulo $x^{2^n} + x$ is:

$$W(x) = \beta \left((x+e)^{2^n-1} + 1 \right).$$

This is simply because the right-hand polynomial above has degree $2^n - 1$ and is equal to W for each x. Thus we proved that

$$P(x) = H(x) + \beta \left((x+e)^{2^n-1} + 1 \right).$$

Since P is a permutation, its degree is at most $2^n - 2$ (from Theorem 5). This implies that H must have the term βx^{2^n-1}; its degree is $2^n - 1$. ◇

Proposition 8 *Let F be defined by (15). Then, F is APN if and only if the polynomial $Q : x \mapsto F(x)/x^2$, i.e.,*

$$Q(x) = \sum_{i=1}^{n-1} c_i x^{2^i-1} \tag{17}$$

is a permutation polynomial on $\mathbf{F}_{2^n}$.

Proof. For any $a \in \mathbf{F}_{2^n}^*$, we have

$$D_a F(x) = \sum_{i=1}^{n-1} c_i \left(x^{2^i} a + x a^{2^i} \right) + F(a) \ .$$

Then, the set $\{D_a F(x), x \in \mathbf{F}_2^n\}$ has cardinality 2^{n-1} if and only if the affine polynomial $D_a F$ has a kernel of dimension 1, i.e.,

$$\sum_{i=1}^{n-1} c_i \left(x^{2^i} a + x a^{2^i} \right) \neq 0 \ \text{ for all } x \notin \{0, a\} \ ,$$

or equivalently (by dividing by xa the polynomial above):

$$\sum_{i=1}^{n-1} c_i x^{2^i-1} \neq \sum_{i=1}^{n-1} a^{2^i-1} \ \text{ for all } x \notin \{0, a\}.$$

That is $Q(x) \neq Q(a)$ for all $x \notin \{0, a\}$. Therefore, F is APN if and only if for any two distinct a and b in $\mathbf{F}_{2^n}^*$, $Q(a) \neq Q(b)$. Moreover, if there exists $a \neq 0$ such that $Q(a) = Q(0) = 0$, this element a is unique. In this case, we know from Lemma 1 that Q has degree $2^n - 1$, which is impossible. Therefore, the previous condition is equivalent to the fact that Q is a permutation polynomial. ◇

Now, using Hermite's criterion, one completely characterizes the permutation polynomials of the form (17). This was actually proved by Payne [26] in another context, the general problem of *the complete determination of all ovoids in the projective plane $PG(2, 2^s)$* (see also [19, Lemma 8.40] and a generalization in [21]). We give here a detailed proof in our context. Our proof requires the following technical lemma.

Lemma 2 *Let n and μ be two positive integers with $\mu < n - 1$ and let $(u_0, \ldots, u_\mu)$ and $(a_0, \ldots, a_\mu)$ be two words of length $\mu + 1$ with components in the range $[1, n-1]$, such that all u_i are distinct. Let u and v be the integers defined by*

$$u = \sum_{i=0}^{\mu} 2^{u_i} \quad \textit{and} \quad v = \sum_{i=0}^{\mu} 2^{a_i + u_i} \ .$$

Then,

$$x^{v-u} \equiv x^{2^n-1} \pmod{x^{2^n} + x} \ \textit{in } \mathbf{F}_{2^n}[x] \ ,$$

if and only if

$$\{a_i + u_i \pmod{n},\ i \in [0, \mu]\} = \{u_i,\ i \in [0, \mu]\} \ .$$

Proof. Since $v > u$, the congruence $x^{v-u} \equiv x^{2^n-1} \pmod{x^{2^n}+x}$ is equivalent to

$$x^v \equiv x^u \pmod{x^{2^n}+x} .$$

But, we have

$$x^v \equiv \prod_{i=0}^{\mu} x^{2^{a_i+u_i \pmod n}} \equiv x^{v'} \pmod{x^{2^n}+x}$$

where $v' = \sum_{i=0}^{\mu} 2^{a_i+u_i \pmod n}$. Therefore, $x^v \equiv x^u$ if and only if both sets

$$\{a_i + u_i \pmod n,\ i \in [0,\mu]\} \text{ and } \{u_i,\ i \in [0,\mu]\}$$

are equal. Indeed, both sets have the same cardinality, otherwise the congruence $x^{v'} \equiv x^u$ does not hold. ◇

By applying the previous lemma with $\mu = 1$, we deduce a first necessary condition for a polynomial Q of the form (17) to be a permutation polynomial.

Proposition 9 *Let*

$$Q(x) = \sum_{i=1}^{n-1} c_i x^{2^i-1},\ \ c_i \in \mathbf{F}_{2^n} .$$

If Q is a permutation polynomial on $\mathbf{F}_{2^n}$, then for all k, $0 < k < n$, at least one element in the pair (c_k, c_{n-k}) is zero.

Proof. We use Hermite's criterion (Theorem 5) with $t = 2^k + 1$, $k \in [1, n-1]$. We have

$$Q^{2^k+1}(x) = \sum_{i=1}^{n-1}\sum_{j=1}^{n-1} c_i^{2^k} c_j x^{2^{i+k}+2^j-2^k-1} .$$

Let $m_{i,j}(x) = x^{2^{i+k}+2^j-2^k-1}$. The monomial $m_{i,j}$ has degree $2^n - 1$ if and only if

$$x^{2^{i+k}+2^j-2^k-1} \equiv x^{2^n-1} \pmod{x^{2^n}+x} .$$

Now, we use Lemma 2 with $\mu = 1$, $(u_0, u_1) = (0, k)$ and $(a_0, a_1) = (j, i)$, i.e., $u = 2^k + 1$ and $v = 2^j + 2^{i+k}$. We deduce that $m_{i,j}$ has degree $2^n - 1$ if and only if $\{0, k\} = \{j, i+k \pmod n\}$. This situation occurs only when $i + k = n$ and $j = k$. Therefore, the only term of degree $2^n - 1$ of Q^{2^k+1} has coefficient $c_{n-k}^{2^k} c_k$. It follows that this term vanishes for any $k \in [1, n-1]$ when Q is a permutation polynomial. ◇

Now, we can prove the general theorem.

Theorem 6 *A polynomial of* $\mathbf{F}_{2^n}[x]$ *of the form*

$$Q(x) = \sum_{i=1}^{n-1} c_i x^{2^i-1}, \quad c_i \in \mathbf{F}_{2^n}$$

cannot be a permutation polynomial unless $Q(x) = cx^{2^k-1}$ *with* $\gcd(k,n) = 1$ *and* $c \in \mathbf{F}_{2^n}^*$.

Consequently, a quadratic function F *over* $\mathbf{F}_{2^n}$ *of the form (15) is APN if and only if* $F(x) = cx^{2^k+1}$ *with* $\gcd(k,n) = 1$ *and* $c \in \mathbf{F}_{2^n}^*$.

Proof. Let $k \in [1, n-1]$ be such that $c_k \neq 0$. Let $r = n-1$ if $\gcd(k,n) = 1$ and $r_k = n/\gcd(k,n)$ otherwise. We will prove by induction on μ that

$$c_{-\mu k} = 0 \quad \text{for all } \mu \in [1, r_k - 1], \tag{18}$$

where all indices are defined modulo n. From the previous proposition, Equation (18) holds for $\mu = 1$. Now, let $\mu < r_k$. We assume that $c_{-\mu' k} = 0$ for any $1 \leq \mu' \leq \mu - 1$, and we are going to prove that $c_{-\mu k} = 0$. Let $u = \sum_{j=0}^{\mu} 2^{kj \pmod n}$. We have

$$\begin{aligned} Q^u(x) &= \left(\sum_{i=1}^{n-1} c_i x^{2^i-1}\right)^{\sum_{j=0}^{\mu} 2^{kj}} \\ &= \prod_{j=0}^{\mu} \left(\sum_{i=1}^{n-1} c_i x^{2^i-1}\right)^{2^{kj}} \\ &= \prod_{j=0}^{\mu} \sum_{i=1}^{n-1} c_i^{2^{kj}} x^{2^{kj+i}-2^{kj}} \\ &= \sum_{a \in [1,n-1]^{\mu+1}} \left(\prod_{j=0}^{\mu} c_{a_j}^{2^{kj}}\right) m_a(x) \end{aligned}$$

where

$$m_a(x) = x^{\sum_{j=0}^{\mu} 2^{kj+a_j} - 2^{kj}}$$

and $a = (a_0, \ldots, a_\mu)$, $a_j \in [1, n-1]$. From Lemma 2, we deduce that the values of a for which m_a has degree $(2^n - 1)$ are those such that

$$\{a_j + kj \pmod n, j \in [0, \mu]\} = \{kj \pmod n, j \in [0, \mu]\}$$

or equivalently those such that

$$a_j = k(\sigma(j) - j) \pmod n, \quad \text{for all } j \in [0, \mu]$$

for some permutation σ of $[0,\mu]$. Since the corresponding monomials m_a have coefficients

$$b_\sigma = \prod_{j=0}^{\mu} c_{k(\sigma(j)-j)}^{2^{kj}} \ ,$$

we deduce that the coefficient of the term of degree (2^n-1) in Q^u is equal to

$$\sum_{\sigma\in\mathcal{S}'_\mu} b_\sigma = \sum_{\sigma\in\mathcal{S}'_\mu} \prod_{j=0}^{\mu} c_{k(\sigma(j)-j)}^{2^{kj}} \ ,$$

where $\mathcal{S}'_\mu$ denotes the group of permutations of $[0,\mu]$ such that $k(\sigma(j)-j) \not\equiv 0 \bmod n$ for all j. Obviously, for any $\sigma\in\mathcal{S}'_\mu$, we have $\sum_{j=0}^{\mu}(\sigma(j)-j)=0$. Since $\sigma(j)\neq j$ for all $j\in[0,\mu]$, there exists at least one index $j\in[0,\mu]$ such that $\sigma(j)-j<0$. If there exists a j such that $-(\mu-1)\leq\sigma(j)-j<0$, the corresponding coefficient b_σ is a multiple of $c_{-k(j-\sigma(j))}$, which vanishes by induction hypothesis. Otherwise, the only j for which $\sigma(j)-j<0$ satisfies $\sigma(j)-j\leq-\mu$. Therefore, σ corresponds to the following permutation

$$\begin{array}{lccccccc} j & = & 0 & 1 & 2 & \ldots & \mu-1 & \mu \\ \sigma(j) & = & 1 & 2 & 3 & \ldots & \mu & 0 \end{array}$$

Moreover, this permutation σ belongs to $\mathcal{S}'_\mu$ because $k(\sigma(j)-j)\not\equiv 0 \bmod n$ since $\mu < n/\gcd(k,n)$. Therefore, the coefficient of degree (2^n-1) of Q^u is

$$\prod_{j=0}^{\mu-1} c_k^{2^{kj}} c_{-\mu k}^{2^{k\mu}} \ .$$

Since u is even, Hermite's criterion then implies that $c_{-\mu k}=0$ if Q is permutation polynomial.

Therefore, we have proved by induction that $c_{-\mu k}=0$ for all $\mu\in[1,r_k-1]$. Then,

- if $\gcd(n,k)=1$, we have

  $$\{-\mu k \pmod n,\ \mu\in[1,n-2]\} = \{1,\ldots,n-1\}\setminus\{k\} \ ,$$

  implying that $Q(x)=c_k x^{2^k-1}$;
- if $\gcd(n,k)=d>1$, we have proved that $c_{-(r_k-1)k}=0$ where $n=r_k\gcd(k,n)$. Therefore, $-k(r_k-1)\equiv k \bmod n$, implying that $c_k=0$ which is a contradiction.

$\diamond$

5 Conclusion

During this work, our main purpose was to tackle several open problems on APN functions. Our main results have concern with nonlinearity, APN permutations and quadratic APN functions. Despite these results, we point out that a number of interesting problems remain open and that these are difficult problems. Among those open issues, one of the most important ones from a cryptographic point of view is the existence of APN permutations depending on an even number of variables. We want to mention also (in the even case) that our result on the nonlinearity of APN power functions is conjectured to be true for any power function, for a long time. In the last part of this paper, we emphasize that the theoretical study of quadratic functions remains of great interest.

References

[1] T. Bending and D. Fon der Flass. Crooked functions, bent functions, and distance regular graphs. *Electron. J. Combin.*, 5(1), 1998. R34.

[2] T.P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy. On Almost Perfect Nonlinear functions. In *Proceedings 2005 IEEE International Symposium on Information Theory, ISIT 05*, Adelaide, Australia, September 2005.

[3] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.

[4] L. Budaghyan, C. Carlet, P. Felke, and G. Leander. An infinite class of quadratic APN functions which are not equivalent to power mappings. Cryptology ePrint Archive, Report 2005/359, 2005. `http://eprint.iacr.org/`.

[5] L. Budaghyan, C. Carlet, and A. Pott. New constructions of Almost Bent and Almost Perfect Nonlinear polynomials. In *Workshop on Coding and Cryptography – WCC 2005*, pages 306–315, Bergen, Norway, March 2005.

[6] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine. Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions. In *Advances in Cryptology - EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 507–522, Berlin, Germany, 2000. Springer-Verlag.

[7] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine. On cryptographic properties of the cosets of $R(1,m)$. *IEEE Transactions on Information Theory*, 47(4):1494–1513, 2001.

[8] A. Canteaut, P. Charpin, and H. Dobbertin. Binary m-sequences with three-valued crosscorrelation: A proof of Welch conjecture. *IEEE Trans. Inform. Theory*, 46(1):4–8, 2000.

[9] A. Canteaut, P. Charpin, and H. Dobbertin. Weight divisibility of cyclic codes, highly nonlinear functions on GF(2^m) and crosscorrelation of maximum-length sequences. *SIAM J. Discrete Math.*, 13(1):105–138, 2000.

[10] C. Carlet. Partially-bent functions. *Des. Codes Cryptogr.*, (3):135–145, 1993.

[11] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes Cryptogr.*, 15(2):125–156, 1998.

[12] L. Carlitz. Explicit evaluation of certain exponential sums. *Math. Scand.*, 44:5–16, 1979.

[13] F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis. In *Advances in Cryptology - EUROCRYPT'94*, volume 950 of *Lecture Notes in Computer Science*, pages 356–365, Berlin, Germany, 1995. Springer-Verlag.

[14] P. Charpin, T. Helleseth, and V. Zinoviev. Propagation characteristics of $x \mapsto x^{-1}$ and Kloosterman sums. *Finite Fields and Appl.*, 2005. To appear.

[15] P. Charpin, A. Tietäväinen, and V. Zinoviev. On binary cyclic codes with minimum distance $d = 3$. *Problems Inform. Transmission*, 33(4):287–296, 1997.

[16] H. Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: a new class for n divisible by 5. In *Proceedings of Finite Fields and Applications Fq5*, pages 113–121, Augsburg, Germany, 2000. Springer-Verlag.

[17] Y. Edel, G. Kyureghyan, and A. Pott. A new APN function which is not equivalent to a power mapping. Preprint, 2005. `http://arxiv.org/abs/math.CO/0506420`.

[18] T. Helleseth. Some results about the cross-correlation function between two maximal linear sequences. *Discrete Mathematics*, 16:209–232, 1976.

[19] J.W.P. Hirschfeld. *Projective Geometries over Finite Fields.* Oxford Mathematical Monographs. Clarendon Press, second edition, 1998.

[20] X.-D. Hou. Affinity of permutations of $\mathbf{F}_2^n$. In *Workshop on Coding and Cryptography – WCC 2003*, pages 273–280, Versailles, France, 2003.

[21] X.-D. Hou. Solution to a problem of Payne. Proceedings of the AMS, Vol. 132, n. 1, pp. 1-6.

[22] R. Lidl and H. Niederreiter. *Finite fields.* Cambridge University Press, 1983.

[23] K. Nyberg. Differentially uniform mappings for cryptography. In *Advances in Cryptology - EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 55–64, Berlin, Germany, 1993. Springer-Verlag.

[24] K. Nyberg. S-boxes and round functions with controllable linearity and differential uniformity. In *Fast Software Encryption - FSE'94*, volume 1008 of *Lecture Notes in Computer Science*, pages 111–130. Springer-Verlag, 1995.

[25] K. Nyberg and L.R. Knudsen. Provable security against differential cryptanalysis. In *Advances in Cryptology - CRYPTO'92*, volume 740 of *Lecture Notes in Computer Science*, pages 566–574. Springer-Verlag, 1993.

[26] S.E. Payne. A complete determination of translation ovoids in finite Desarguian planes. *Lincei - Rend. Sc. fis. mat. e nat.*, LI, November 1971.

[27] E.R. van Dam and D. Fon der Flass. Codes, graphs, and schemes from nonlinear functions. Technical report, Research memorandum, FEW 790, Tilburg University, The Netherlands, May 2000.

[28] X.-M. Zhang and Y. Zheng. GAC - the criterion for global avalanche characterics of cryptographic functions. *Journal of Universal Computer Science*, 1(5):320–337, 1995.

[29] Y. Zheng and X.-M. Zhang. Plateaued functions. In *Information and Communication Security, ICICS'99*, volume 1726 of *Lecture Notes in Computer Science*, pages 224–300. Springer-Verlag, 1999.

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)

Unité de recherche INRIA Lorraine : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38330 Montbonnot-St-Martin (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399